

⑫ 公開特許公報(A)

平4-43734

⑬ Int. Cl.³

識別記号

庁内整理番号

⑭ 公開 平成4年(1992)2月13日

H 04 L 9/32
G 06 F 15/00
H 04 L 12/22

3 3 0 B

7218-5L

7117-5K
7830-5K

H 04 L 9/00
11/26

A

審査請求 未請求 請求項の数 1 (全6頁)

⑮ 発明の名称 対話型個人認証装置

⑯ 特 願 平2-151840

⑰ 出 願 平2(1990)6月11日

⑱ 発 明 者 宮 内 直 人 神奈川県鎌倉市大船5丁目1番1号 三菱電機株式会社情報電子研究所内

⑲ 出 願 人 三菱電機株式会社 東京都千代田区丸の内2丁目2番3号

⑳ 代 理 人 弁理士 宮園 純一

明 細 書

1. 発明の名称

対話型個人認証装置

2. 特許請求の範囲

ネットワーク上のコンピュータの利用者を識別する対話型個人認証装置において、利用者の名前などを示す識別子とそのパスワードを対にして予め記憶する第1記憶部と、利用者から入力した識別子を上記第1記憶部に記憶された識別子と比較することにより、識別する名前識別部と、上記第1記憶部に記憶された利用者のパスワードをランダムに変更して合成パスワードを発生する合成パスワード発生部と、上記第1記憶部に記憶された利用者のパスワードと上記合成パスワードとの差分である合成認証情報を記憶する第2記憶部と、利用者から送られてきた合成認証情報と上記第2記憶部に記憶された合成認証情報とを比較し利用者の認証を行う認証識別部とを備えたことを特徴とする対話型個人認証装置。

3. 発明の詳細な説明

(産業上の利用分野)

この発明はネットワーク上のコンピュータへアクセスする場合の利用者の認証を行う対話型個人認証装置に関するものである。

(従来の技術)

従来、この種の対話型個人認証方法としては例えば、

カール、H.マイアー、スティーブソン、M.マティス共著

「暗号」自然社(昭61-2-10)p.358-p.394

D.H.Davies, W.L.Price共著

「ネットワークセキュリティ」日経マグローヒル社(昭60-12-5)p.111-p.132

小林、山本

「5U-7 ソフトウェアの権利保護のためのアクセス制御方式」「第33回全国大会講演論文集」情報処理学会(昭61-10-1)p.1097-p.1098

CCITT

「Recommendation X.509 The Directory-Authentication Framework」(1988-12)p.12-p.14

に示されたようなものがあった。

第5図は従来の対話型個人認証装置の構成を示すブロックである。第5図において、51は利用者の認証を行う認証サーバである。この認証サーバ51は、認証クライアント56から利用者の識別子とそのパスワードを入力したりするサーバ側入出力部52と、利用者の識別子とそのパスワードを対にして記憶する第1記憶部55と、サーバ側入出力部52によって入力された利用者の識別子を第1記憶部55に記憶されている利用者の識別子と比較し利用者の名前の妥当性を評価する名前識別部53と、サーバ側入出力部52によって入力された利用者のパスワードを第1記憶部55に記憶されている利用者のパスワードと比較し認証情報の妥当性を評価する認証識別部54とを備えている。認証クライアント56は、認証サーバ51に対して認証操作を行うクライアントである。クライアント側入出力部57は、利用者が識別子とパスワードを入力し、これらを認証サーバ51へ送信するものである。伝送路58は利用者の識

別子とパスワードを伝送するためのものである。

次にこの従来例の動作を第6図のフローチャートを参照して説明する。まず、ステップ61でサーバ側入出力部52から利用者の識別子N1とパスワードP1を入力する。次にステップ62で名前識別部53がステップ61で入力された識別子Nと第1記憶部55に登録（記憶されている識別子N0と）を比較し両者が同一ならばステップ63を実行し、異なる場合は認証不正となり処理を終了する。ステップ63では入力した識別子N0に対応するパスワードP1を第1記憶部55から取得する。次にステップ64で認証識別部54が入出力部52から入力したパスワードP0を第1記憶部55に登録されているパスワードP1と比較し両者が同一ならば認証が正常に終了する。両者が異なる場合は認証不正となり処理を終了する。

このように、従来の対話型個人認証装置は、利用者を識別するために、サーバ側入出力部52から識別子とパスワードを入力し、第1記憶部55に記憶されている識別子とパスワードを比較する

ことによって、利用者の認証を行うように構成されている。

〔発明が解決しようとする課題〕

以上のような従来の対話型個人認証装置は、利用者の識別子とパスワードによって、暗号技術を使った認証よりも簡易に認証を行えるが、ネットワークの伝送路上に利用者の識別子とパスワードが流れるため、それらが盗聴されるおそれがあり、また、盗聴防止のためには暗号化処理を行う方法もあるが、従来の方法は処理が複雑であるという問題点があった。

この発明は上記のような問題点を解決するためになされたもので、高度な暗号化技術を使わなくても、登録されているパスワードが伝送路上から盗聴されることを防ぐことができる対話型個人認証装置を提供することを目的とする。

〔課題を解決するための手段〕

この発明に係る対話型個人認証装置は、利用者の名前などを示す識別子とそのパスワードを対にして予め記憶する第1記憶部5と、利用者から入

力した識別子を第1記憶部5に記憶された識別子と比較することにより識別する名前識別部3と、第1記憶部5に記憶された利用者のパスワードをランダムに変更して合成パスワードを発生する合成パスワード発生部7と、第1記憶部5に記憶された利用者のパスワードと上記合成パスワードとの差分である合成認証情報を記憶する第2記憶部6と、利用者から送られてきた合成認証情報と第2記憶部6に記憶された合成認証情報とを比較し利用者の認証を行う認証識別部4とを備えたものである。

〔作用〕

第1記憶部5は利用者の識別子とそのパスワードを対にして予め記憶する。名前識別部3は、利用者から入力した識別子を、第1記憶部5に記憶された識別子と比較することにより識別する。合成パスワード発生部7は第1記憶部5に記憶された利用者のパスワードをランダムに変更して合成パスワードを発生する。第2記憶部6は利用者のパスワードと合成パスワードとの差分である合成認

証情報を記憶する。認証識別部4は利用者から送られてきた合成認証情報と第2記憶部6に記憶されている合成認証情報とを比較し利用者の認証を行う。

(実施例)

第1図はこの発明の一実施例に係る対話型個人認証装置の構成を示すブロック図である。第1図において、1は利用者の認証を行う認証サーバである。認証サーバ1は認証クライアント8から利用者の識別子と合成認証情報を入力し認証クライアント8に合成パスワードを出力するサーバ側入出力部2と、このサーバ側入出力部2から入力した利用者の名前などを示す識別子を第1記憶部5に記憶された識別子と比較することにより識別する名前識別部3と、サーバ側入出力部2より入力した利用者からの合成認証情報と第2記憶部6に記憶された合成認証情報とを比較し利用者の認証を行う認証識別部4と、利用者の識別子とそのパスワードを対にして予め記憶する第1記憶部5と、第1記憶部5に記憶された利用者のパスワードと

合成パスワードとの差分である合成認証情報を記憶する第2記憶部6と、第1記憶部5に記憶された利用者のパスワードをランダムに変更して合成パスワードを発生する合成パスワード発生部7とを備えている。認証クライアント8は、認証サーバ1に対して認証操作を行うクライアントであり、利用者の識別子と合成認証情報を入力してこれらを認証サーバ1に送信し、また、認証サーバ1から入力した合成パスワードを利用者に出力するクライアント側入出力部9を備えている。伝送路10は、認証サーバ1と認証クライアント8間で、利用者の識別子、合成パスワード、合成認証情報などを伝送するものである。

第2図は認証サーバ1が利用者の認証を行う際の手続きを示すフローチャートで、第3図は認証クライアント8が利用者の認証手続きを行う際のフローチャートである。

次にこの実施例の動作について第1図～第3図を参照して説明する。

まず、第3図において、ステップ21でクライ

アント側入出力部9が、利用者から識別子N1を入力する。次に、ステップ22でクライアント側入出力部9が、認証サーバ1に利用者の識別子N1を出力する。

次に、第2図において、ステップ11で、サーバ側入出力部1が認証クライアント8から利用者の識別子N1を入力する。次に、ステップ12で名前識別部3はステップ11で入力した利用者の識別子N1を第1記憶部5に登録されている利用者の識別子N0と比較し、利用者の識別子N1の正誤を判別する。利用者の識別子N1が正しければ、ステップ13を実行する。次にステップ13で、ステップ12で入力した識別子N1と対をなすパスワードP0を第1記憶部5から検索する。次にステップ14で、合成パスワード発生部7が、パスワードP0を基に合成パスワードP1を生成する。次に、ステップ15で、ステップ14で得られた合成パスワードP1とステップ13で得られたパスワードP0の差分の文字列を合成認証情報D0として、第2記憶部6に記憶する。次に、

ステップ16で、ステップ15で得られた合成パスワードP1をサーバ側入出力部2から伝送路10を通して、認証クライアント8に出力する。

次に第3図において、ステップ23で、認証クライアント8のクライアント側入出力部9において、認証サーバ1から合成パスワードP1を入力する。次に、ステップ24でクライアント側入出力部9が利用者に合成パスワードP1を出力する。次に、ステップ25で、クライアント側入出力部9が利用者から合成認証情報D1を入力する。この時、合成認証情報D1は、利用者が記憶しているパスワードと合成パスワードの差分である。次に、ステップ26で、認証クライアント8のクライアント側入出力部9において、ステップ25で得られた合成認証情報D1を伝送路10を通して認証サーバ1に出力する。

次に、第2図において、ステップ17で、認証サーバ1のサーバ側入出力部2において、認証クライアント8から合成認証情報D1を入力する。ステップ18で、認証識別部4がステップ17で

入力した合成認証情報D1とステップ15で記憶した合成認証情報D0を比較する。比較結果が正しければ、利用者の認証を完了する。

このようにして、伝送路10に利用者のパスワードを流すことなく、また複雑な暗号手法を使わずに、ネットワークにおける盗聴を回避できる。

第4図は他の実施例の構成を示すブロック図であり、第4図において第1図に示す構成要素に対応するものには同一の符号を付し、その説明を省略する。第4図において、41は認証クライアント8に備えられるパスワード変換部である。第1図の実施例では、認証クライアント8のクライアント側入出力部9が利用者から合成認証情報D1を入力して認証を行うものについて説明したが、第4図の実施例の場合、利用者は従来通りのパスワードP2を認証クライアント8に入力し、パスワード変換部41がそのパスワードP2と認証サーバ1から送られてくる合成パスワードP1とを比較して、合成認証情報D1を生成する。このようにすれば、第1の実施例と同様の効果がある

を行い、伝送路10上にパスワードを送信しないため、伝送路10におけるパスワードの盗聴を防止することができる。

(発明の効果)

以上のように本発明によれば、利用者のパスワードをランダムに変更して合成パスワードを生成し、利用者のパスワードと合成パスワードとの差分である合成認証情報を記憶させ、この記憶された合成認証情報と利用者から送られてきた合成認証情報とを比較することにより、利用者の認証を行うように構成したので、高度な暗号化技術を使わなくても、登録されているパスワードが伝送路上から盗聴されることが防止でき、これにより、従来のパスワードによる認証よりも安全性が高まる上、利用者はパスワードの他に認証情報を覚える必要がなく、従来の暗号化技術よりも容易にパスワードを隠蔽できるという効果が得られる。

4. 図面の簡単な説明

第1図はこの発明の一実施例に係る対話型個人認証装置の構成を示すブロック図、第2図は第1

のに加え、利用者インタフェースに従来の認証手段と同じものが使用できるため、利用者から新しい認証手段を隠蔽できるという効果がある。

以上説明したように上記各実施例は、利用者の識別子をサーバ側入出力部2から入力し、この入力した識別子と第1記憶部5に記憶されている識別子とを名前識別部3で比較し、合成パスワード発生部7で識別子と対になっているパスワードをランダムに合成し、この合成したパスワードと第1記憶部5に記憶されているパスワードとの差分を合成認証情報として第2記憶部6に記憶し、サーバ側入出力部2においてその合成パスワードを認証クライアント8に出力し、また、認証クライアント8を通じて利用者から合成認証情報を入力し、認証識別部4において、入力した合成認証情報と第2記憶部6に記憶されている合成認証情報とを比較し、その結果により利用者の認証を行うように構成されている。

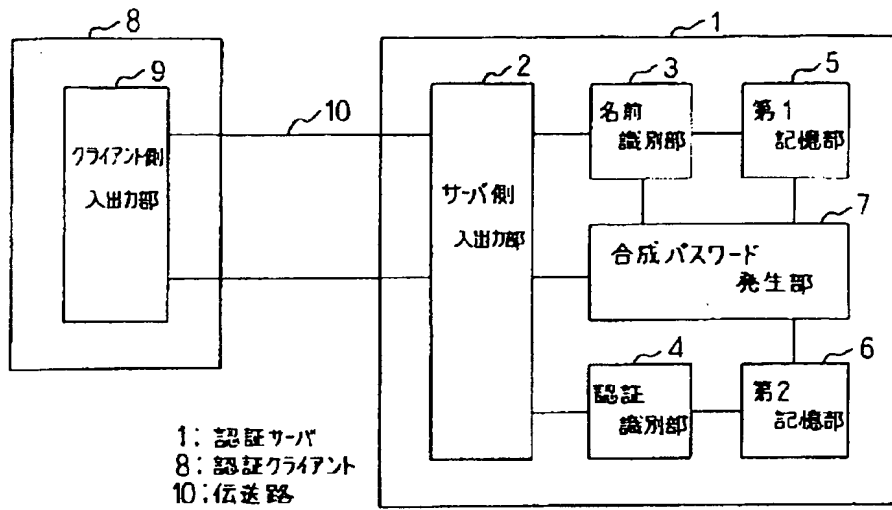
上記各実施例によれば、認証のために認証サーバ1と認証クライアント8間で2往復のアクセス

図中の認証サーバが利用者の認証を行う際の手続きを示すフローチャート、第3図は第1図中の認証クライアントが利用者の認証手続きを行う際のフローチャート、第4図は他の実施例に係る対話型個人認証装置の構成を示すブロック図、第5図は従来の対話型個人認証装置の構成を示すブロック図、第6図はこの従来装置の認証動作を示すフローチャートである。

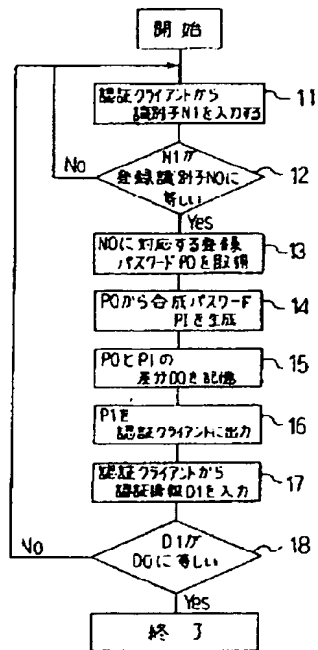
3・・・名前識別部、4・・・認証識別部、5・・・第1記憶部、6・・・第2記憶部、7・・・合成パスワード発生部。

代理人 弁理士 宮 園 純 一

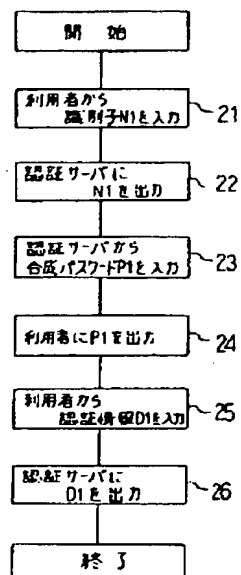
第 1 図



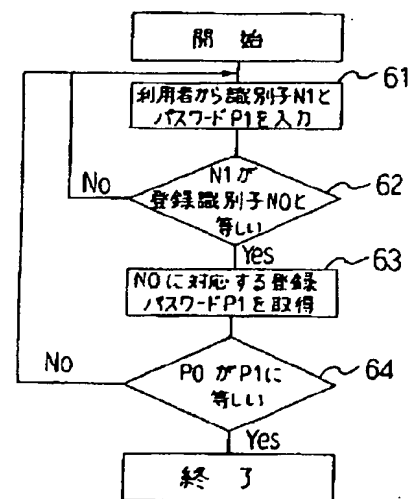
第 2 図



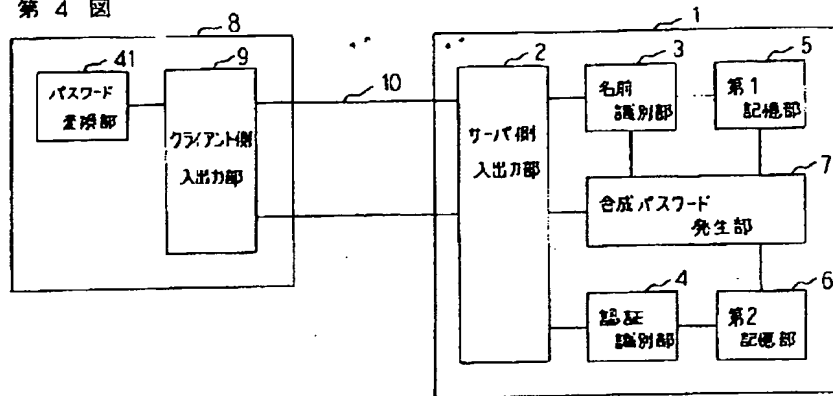
第 3 図



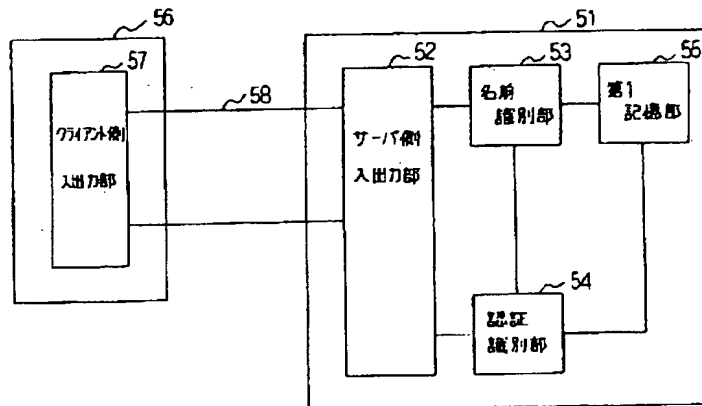
第 6 図



第 4 図



第 5 図



手 続 補 正 書 (自発)

平成 2 年 7 月 27 日

特許庁長官殿

1. 事件の表示 特願平2-151840号

2. 発明の名称

対 話 型 個 人 認 証 装 置

3. 補正をする者

事件との関係 特許出願人
住 所 東京都千代田区丸の内二丁目2番3号
名 称 (601)三菱電機株式会社
代表者 志 枝 守 哉

4. 代 理 人

住 所 東京都千代田区飯田橋二丁目9番4-405
宮園国際特許事務所
氏 名 (802B)弁理士 宮 園 純
(連絡先03(234)5650)三平

5. 補正の対象

明細書の発明の詳細な説明の欄。

6. 補正の内容

(1)明細書の第4頁第7行目「登録(記憶されている)」とあるのを「登録(記憶)されている」と補正する。

以 上

方 式 査 査

関 川

